JUNOS Software with Enhanced Services 9.2 for J-series Services Router Release Notes

Release 9.2R4
May 2009
Part Number: 530–025667–01
Revision 4

These release notes accompany Release 9.2R4 of JUNOS software with enhanced services for J-series Services Routers. They briefly describe new software and hardware features and provide a summary of the current software limitations and known defects that exist in this release.

NOTE: J-series Services Routers are currently shipped with the JUNOS software. To install JUNOS software with enhanced services on your Services Router, see the *JUNOS Software Migration Guide*. The *J-series Services Router Quick Start* is shipped with the router. You can download the *J Series Services Routers Quick Start* from the Juniper Web site at http://www.juniper.net/techpubs/.

You can also find these release notes on the Juniper Networks Technical Publications Web page located at http://www.juniper.net/techpubs/.

Contents

JUNOS Software with Enhanced Services Features 3
Interfaces and Chassis 3
J-Web User Interface 3
Software Installation and Upgrade 4
JUNOS Features Not Supported for Chassis Clusters 4
Changes in Default Behavior and Syntax 4
Outstanding Issues 5
Resolved Issues 8
Errata 8

Power and Heat Dissipation Requirements for J-series PIMs 9
Supported Third-Party Hardware 9
J-series Compact Flash and Memory Requirements 10
JUNOS Software with Enhanced Services Upgrade and Downgrade Instructions 10
Upgrade and Downgrade Overview 11
Upgrade Software Packages 11
Recovery Software Packages 12
Before You Begin 12
Downloading Software Upgrades from Juniper Networks 13
Installing Software Upgrades with the J-Web Interface 13
Installing Software Upgrades from a Remote Server 13
Installing Software Upgrades by Uploading Files 14
Installing Software Upgrades with the CLI 15
Installing Software Upgrades by Downloading Files 15
Installing Software Upgrades from a Remote Server 16
Downgrade Instructions 16
Downgrading the Software with the J-Web Interface 17
Downgrading the Software with the CLI 17
List of Technical Publications 18
Documentation Feedback 19
Requesting Technical Support 19
Revision History 21

JUNOS Software with Enhanced Services Features

Release 9.2R4 of JUNOS software with enhanced services includes the following features. For more information, see the following manuals:

- *JUNOS Software Migration Guide*
- *J Series Services Routers Hardware Guide*
- *J Series Services Routers Quick Start*
- *JUNOS Software Design and Implementation Guide*
- *JUNOS Software Interfaces and Routing Configuration Guide*
- *JUNOS Software Administration Guide*
- *JUNOS Software CLI Reference*
- *WXC Integrated Services Module Installation and Configuration Guide*

Interfaces and Chassis

- **Enhanced switching services on Ethernet uPIMs in J2320, 2350, J4350, and J6350 Secure Routers**—For enterprise customers and branch offices who want to eliminate a layer of switching from their network, enterprise-class Ethernet switching support for uPIMs enables integrated Ethernet switching and routing (with WAN connectivity) along with security features in a single box.

J-Web User Interface

- **J-Web Monitor pages for enhanced switching**—The J-Web interface now provides Monitor pages for enhanced switching. New Monitor pages for enhanced switching allow you to monitor information and status for the following:
  - Spanning Tree Protocol (STP)
  - Generic Virtual Local Area Network Registration Protocol (GVRP)
  - Dot1X
- **J-Web GUI change to the new AJAX framework**—The J-Web interface GUI design now provides a new framework. It introduces a new dashboard that fully utilizes the powers of the new AJAX GUI. It allows panel updates instead of page updates. You can set the preferences on the new dashboard to view the system properties.

Software Installation and Upgrade

- **Compact flash optimization**—Previously, upgrading images on J-series routers with a 256-MB compact flash from Release 8.5 onward involved removing unwanted files in the images and removing the Swap Partition. Now, the software accomplishes the upgrade efficiently by using mdimage to take another snapshot of the compact flash, install the image, and restore configurations.

JUNOS Features Not Supported for Chassis Clusters

For this release of JUNOS software with enhanced services, the following features are not supported when chassis clustering is enabled on the router:

- **Packet-based protocols.** All packet-based protocols, such as Multiprotocol Label Switching (MPLS), Connectionless Network Service (CLNS), and IP version 6 (IPv6)
- **Services interfaces functions.** Any function that depends on the configurable J-series services interfaces:
  - ls-0/0/0—Link services Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Compressed Real-Time Transport Protocol (CRTP)
  - gr-0/0/0—Generic routing encapsulation (GRE) and tunneling
  - ip-0/0/0—IP-over-IP (IP-IP) encapsulation
  - pd-0/0/0, pe/0/0/0, and mt-0/0/0—All multicast protocols
  - lt-0/0/0—Real-time performance monitoring (RPM)
- **WXC Integrated Services Module (WXC ISM 200)**
- **Ethernet switching on some PIMs:**
  - 4-port Fast Ethernet ePIMs running in switching mode
  - 8-port and 16-port Gigabit Ethernet uPIMs running in switching mode
- **ISDN BRI**

Changes in Default Behavior and Syntax

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the JUNOS software with enhanced services documentation:

For Security

- J-series Services Routers do not support the authentication order password radius or password ldap in the edit access profile *profile-name* authentication-order command. Instead, use the order radius password or ldap password.

Outstanding Issues

Authentication

- During user authentication, the firewall authentication table in the output of the security firewall-authentication users command displays multiple failures even though the network table in the output of show network-access requests statistics shows successful authentications. [PR/250780]
- Your attempt to log in to the router from a management device through FTP or Telnet might fail if you type your username and password in quick succession before the prompt is displayed, in some operating systems. As a workaround, type your username and password after getting the prompts. [PR/255024]

Chassis Cluster

- In a chassis cluster, the show interface terse command on the secondary routing engine does not display the same details as that of the primary routing engine. [PR/237982]
- Because the clear security alg sip call command triggers a SIP RTO to synchronize sessions in a chassis cluster, use of the command on one node with the node-id, local, or primary option might result in a SIP call being removed from both nodes. [PR/263976]
- In a chassis cluster configuration, after redundancy group 1 fails over to the secondary node, the statistics for the TCP SYN-ACK-ACK proxy screen are still displayed for the primary node rather than the secondary. [PR/264790]
- When a new redundancy group is added to a chassis cluster, the node with lower priority might be elected as primary when the preempt option is not enabled for the nodes in the redundancy group. [PR/265340]
- In a chassis cluster, if you manually fail over redundancy groups to move the system from active-passive mode to active-active mode during an active call, a subsequent call transfer involving the endpoints of the existing call might fail. [PR/265598]
- When you commit a configuration for a node belonging to a chassis cluster, all the redundancy groups might fail over to node 0. If graceful protocol restart is not configured, the failover can destabilize routing protocol adjacencies and disrupt traffic forwarding. To allow the commit operation to take place without causing a failover, we recommend that you use the set chassis cluster heartbeat-threshold 5 command on the cluster. [PR/265801]
- In a chassis cluster, if a forwarding process restart or system reboot triggers a cold synchronization during an active SIP call, the call might stay in both routing nodes even after the endpoints hang up. As a workaround, use the clear security alg sip call command to clear the call. [PR/267696]
- In a chassis cluster, a high load of SIP ALG traffic might result in some call leaks in active resource manager groups and gates on the backup router. [PR/268613]
- In a chassis cluster, CA certificate enrollment from the secondary Routing Engine does not work. As a workaround, enroll the CA certificate from the primary Routing Engine. [PR/278420]

- In a chassis cluster, J-Web does not enable you to configure the address book. We recommend that you use the command-line interface (CLI) to configure the address book. [PR/281986]
- Chassis SNMP objects are not reporting correctly when a Services Router operates in JSRP cluster mode with JUNOS software. [PR/304082]
- You are not able to configure vlan-ids greater than 1023 on reth interfaces on all platforms supporting chassis cluster. [PR/314636]

Class of Service

- J4350 and J6350 Services Routers might not have the requisite data buffers needed to meet expected delay-bandwidth requirements. Lack of data buffers might degrade CoS performance with smaller-sized (500 bytes or less) packets. [PR/73054]
- With a CoS configuration, when you try to delete all the flow sessions using the clear security flow session command, the WX application acceleration platform may fail over with heavy traffic. [PR/273843]

Enhanced switching

- Traffic statistics are not updated on the ae interface. [PR/292749]
- When a native VLAN is removed from a port, it still accepts untagged traffic and untagged traffic is still transmitted out of it. Restarting chassisd corrects this behavior. [PR/299961]
- If the access port is tagged with the same VLAN that is configured at the port, the access port accepts tagged packets and determines the MAC. [PR/302635]
- VLAN output traffic statistics are not being updated. [PR/305845]

Flow

- OSPF over GRE over IPSec does not work. [PR/105279]
- In JUNOS software with enhanced services, the TTL value on the Internet control message protocol (ICMP) responses is set to 65. [PR/233844]
- Even when forwarding options are set to drop packets for the ISO protocol family, the router forms End System-to-Intermediate System (ES-IS) adjacencies and transmits packets because ES-IS packets are Layer 2 terminating packets. [PR/252957]
- When heartbeat signals are sent to an interface at the server side, the counter on that interface does not increment even after considerable wait time. [PR/273901]
- OSPF over a multipoint interface connected as a hub-and-spoke network does not restart when a new path is found to the same destination. [PR/280771]
- On J-series Services Routers, outbound filters will be applied twice for host-generated IPv4 traffic. [PR/301199]

Infrastructure

- You must remove the U3 support before using the device as a boot medium. For the U3 Titanium device, you can use the U3 Launchpad Removal Tool on a Windows-based system to remove the U3 features. The tool is available for download at http://www.sandisk.com/Retail/Default.aspx?CatID=1415. (To restore the U3 features, use the U3 Launchpad Installer Tool accessible at http://www.sandisk.com/Retail/Default.aspx?CatID=1411). [PR/102645]
- If the router does not have an ARP entry for an IP address, it drops the first packet from itself to that IP address. [PR/233867]
- On J2320, J2350, J4350, and J6350 Services Routers, when you press the F10 key to save and exit from BIOS configuration mode, the operation might not work as expected. As a workaround, use the Save and Exit option from the Exit menu. This issue can be seen on the J4350 and J6350 routers with BIOS Version 080011 and on the J2320 and J2350 routers with BIOS Version 080012. [PR/237721]
- On J2320, J2350, J4350, and J6350 Services Routers, the Clear NVRAM option in the BIOS configuration mode does not work as expected. This issue can be seen on the J4350 and J6350 routers with BIOS Version 080011 and on the J2320 and J2350 routers with BIOS Version 080012. To help mitigate this issue, note any changes you make to the BIOS configuration so that you can revert to the default BIOS configuration as needed. [PR/237722]
- If you enable security trace options, the log file might not be created in the default location at /var/log/security-trace. As a workaround, manually set the log file to the directory /var/log/security-trace. [PR/254563]

Interfaces and Chassis

- The link status of the onboard Gigabit Ethernet interfaces (ge-0/0/0 through ge-0/0/3) or the 1-port Gigabit Ethernet ePIM interface on J4350 and J6350 Services Routers fails when you configure these interfaces in loopback mode. [PR/72381]

Routing

- Asymmetric routing, such as tracing a route to a destination behind J-series routers running JUNOS software with enhanced services with Virtual Router Redundancy Protocol (VRRP), does not work. [PR/237589]

System

- The ping status of the generic routing interfaces (gr-x/y/x) connection established through the ISDN simulator fails. As a workaround, deactivate and reactivate the generic routing interfaces. [PR/282588]

VPN

- The proxy-identity statement is valid for route-based VPN configuration only. Policy-based VPN does not support the proxy-identity statement. [PR/296468]

WXC Integrated Services Module

- When two J-series routers with WXC Integrated Services Modules (WXC ISM 200s) installed are configured as peers, traceroute fails if redirect-wx is configured on both peers. [PR/227958]
- JUNOS software with enhanced services does not support policy-based VPN with WXC Integrated Services Modules (WXC ISM200s). [PR/281822]

Resolved Issues

The following issues have been resolved since Release 9.2R3 of JUNOS software with enhanced services. The identifier following the description is the tracking number in our bug database.

ALG

- On J6350 Services Routers handling more than 1000 simultaneous MGCP calls, the success rate for all MGCP ALG calls was approximately 95 percent. [PR/254297: This issue has been resolved.]
- JUNOS software with enhanced services did not have an option for setting default values for Sun RPC and Microsoft RPC applications. [PR/256971: This issue has been resolved.]

Chassis Cluster

- In a chassis cluster, Layer 2 switching did not work for 4-Port Fast Ethernet ePIMs, 8-Port Gigabit Ethernet uPIMS, and 16-Port Gigabit Ethernet uPIMs. [PR/266857: This issue has been resolved.]
- A chassis cluster using Web authentication might display an "invalid username-password" message even though the user was successfully authenticated locally or through authentication servers. [PR/274077: This issue has been resolved.]

Class of Service

- In J2350 Services Routers, CoS did not work when the data sent to the egress ge interface was more than 100 MB. [PR/281367: This issue has been resolved.]

Enhanced switching

- In the case of traffic going through one of the ports of a LAG running LACP, any change in remote port (for example, port going down) did not change the distribution of traffic at the local switch. [PR/292136: This issue has been resolved.]
- Ping failed when the encapsulation was changed on an existing ISDN call. [PR/303759: This issue has been resolved.]

Interface and Chassis

- If the MTU was set to more than 6 KB for a built-in Gigabit Ethernet port or a 1-port Gigabit Ethernet ePIM, packets might be discarded with an FCS error. [PR/82245: This issue has been resolved.]
- If one routing instance type was changed from vrf to virtual router and then changed back to vrf, the mt interface might fail to come up again. [PR/307401: This issue has been resolved.]

Errata

Screens

- The following guides contain incorrect screen configuration instructions:
  - *JUNOS Software Security Configuration Guide*, "Attack Detection and Prevention" chapter
  - *JUNOS Software Design and Implementation Guide*, "Implementing Firewall Deployments for Branch Offices" chapter

Examples throughout both of these guides describe how to configure screen options using the [set security screen *screen-name*] CLI statements. Instead, you should use the [set security screen ids-option *screen-name*] CLI statements. All screen configuration options are located in the [set security screen ids-option *screen-name*] level of the configuration hierarchy.

Power and Heat Dissipation Requirements for J-series PIMs

On J-series Services Routers, the system monitors the PIMs and verifies that the PIMs fall within the power and heat dissipation capacity of the chassis. If power management is enabled and the capacity is exceeded, the system prevents one or more of the PIMs from becoming active.

CAUTION: Disabling power management can result in hardware damage if you overload the chassis capacities.

You can also use CLI commands to choose which PIMs are disabled. For details about calculating the power and heat dissipation capacity of each PIM and troubleshooting procedures, see the *J Series Services Routers Hardware Guide*.

Supported Third-Party Hardware

The following third-party hardware is supported for use with J-series Services Routers running JUNOS software with enhanced services.

USB Modem We recommend using a Multi-Tech MultiModem MT5634ZBA-USB-V92 USB modem with J-series Services Routers.

Storage Devices The USB slots on J-series Services Routers accept a USB storage device or USB storage device adapter with a compact flash disk installed, as defined in the CompactFlash Specification published by the CompactFlash Association. When the USB device is installed and configured, it automatically acts as a secondary boot device if the primary compact flash disk fails on startup. Depending on the size of the USB storage device, you can also configure it to receive any core files generated during a router failure. The USB device must have a storage capacity of at least 256 MB.

Table 1 on page 9 lists the USB and compact flash storage devices supported for use with the J-series Services Routers.

Table 1: Supported Storage Devices on the J-series Services Routers

Manufacturer	Storage Capacity	Third-Party Part Number
SanDisk—Cruzer Mini 2.0	256 MB	SDCZ2-256-A10
SanDisk	512 MB	SDCZ3-512-A10
SanDisk	1024 MB	SDCZ7-1024-A10

Table 1: Supported Storage Devices on the J-series Services Routers *(continued)*

Manufacturer	Storage Capacity	Third-Party Part Number
Kingston	512 MB	DTI/512KR
Kingston	1024 MB	DTI/1GBKR
SanDisk—ImageMate USB 2.0 Reader/Writer for CompactFlash Type I and II	N/A	SDDR-91-A15
SanDisk CompactFlash	512 MB	SDCFB-512-455
SanDisk CompactFlash	1 GB	SDCFB-1000.A10

J-series Compact Flash and Memory Requirements

Table 2 on page 10 lists the compact flash and DRAM requirements for J-series Services Routers.

Table 2: J-series Compact Flash and DRAM Requirements

Model	Minimum Compact Flash Required	Minimum DRAM Required	Maximum DRAM Supported
J2320	512 MB	512 MB	1 GB
J2350	512 MB	512 MB	1 GB
J4350	512 MB	512 MB	2 GB
J6350	512 MB	1 GB	2 GB

JUNOS Software with Enhanced Services Upgrade and Downgrade Instructions

NOTE: This information applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software Migration Guide*.

In JUNOS Release 8.5, the JUNOS software was extended to use FreeBSD version 6.1. As a result, the following requirements apply when you upgrade your router to JUNOS Release 8.5 and later:

- To upgrade with the JUNOS CLI, the minimum requirement for installation media (such as a compact flash disk, internal flash disk, or PC card) is 512 MB. To use the J-Web interface for an upgrade, you must have 512 MB or more.

- Before upgrading to JUNOS software with enhanced services, perform the following:
  - Upgrade to a 512-MB compact flash. For upgrading the DRAM module or compact flash, see the "Upgrading the DRAM Module or Compact Flash" section of the *JUNOS Software Migration Guide*. For information on formatting a new, blank compact flash card, see the "Configuring Internal Compact Flash Recovery" section of the *JUNOS Software Administration Guide*.

This section contains the following topics:

- Upgrade and Downgrade Overview on page 11
- Before You Begin on page 12
- Downloading Software Upgrades from Juniper Networks on page 13
- Installing Software Upgrades with the J-Web Interface on page 13
- Installing Software Upgrades with the CLI on page 15
- Downgrade Instructions on page 16

Upgrade and Downgrade Overview

Typically, you upgrade JUNOS software with enhanced services on a Services Router by downloading a set of images onto your router or onto another system on your local network, such as a PC. You then uncompress the package and install the uncompressed software using the CLI. Finally, you boot your system with this upgraded device.

A JUNOS software package is a collection of files that make up a software component. You can download software packages either for upgrading JUNOS software or for recovering a primary compact flash.

All JUNOS software and JUNOS software with enhanced services is delivered in signed packages that contain digital signatures, Secure Hash Algorithm (SHA-1) checksums, and Message Digest 5 (MD5) checksums. For more information about signed software packages, see the *JUNOS Software Installation and Upgrade Guide*.

Upgrade Software Packages

Download an upgrade software package, also known as an install package, to install new features and software fixes as they become available.

An upgrade software package name is in the following format: *package-name-m.nZx.y-distribution.tgz*.

- *package-name* is the name of the package—for example, junos-jsr.
- *m.n* is the software release, with *m* representing the major release number—for example, 9.0.
- *Z* indicates the type of software release. For example, R indicates released software, and B indicates beta-level software.

- *x.y* represents the version of the major software release—for example, 1.1.
- *distribution* indicates the area for which the software package is provided—domestic for the United States and Canada and export for worldwide distribution.

A sample JUNOS software with enhanced services package name is junos-jsr-9.2R4.1-domestic.tgz.

Recovery Software Packages

Download a recovery software package, also known as an install media package, to recover a primary compact flash device.

A recovery software package name is in the following format: *package-name-m.nZx-export-cfnnn.gz*.

- *package-name* is the name of the package—for example, junos-jsr.
- *m.n* is the software release, with *m* representing the major release number—for example, 8.5.
- *Z* indicates the type of software release. For example, R indicates released software, and B indicates beta-level software.
- *x* represents the version of the major software release—for example, 1.
- export indicates that the recovery software package is the exported worldwide software package version.
- *cfnnn* indicates the size of the target compact flash device in megabytes—for example, cf256.

A sample JUNOS software with enhanced services recovery package name is junos-jsr-8.5R1-export-cf256.gz.

Before You Begin

Before upgrading, be sure to back up the currently running and active file system and configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. To back up the file system, you must have a removable compact flash disk installed on a J2320 or J2350 Services Router, or a USB drive installed on any J-series Services Router. The backup device must have a storage capacity of at least 256 MB.

To back up the file system to the removable compact flash disk, issue the following command:

```
user@host> request system snapshot media removable-compact-flash
```

To back up the file system to the removable USB drive, issue the following command:

```
user@host> request system snapshot media usb
```

Downloading Software Upgrades from Juniper Networks

Follow these steps to download software upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks Web page. Depending on your location, select either **Canada and U.S. Version** or **Worldwide Version**:
   - https://www.juniper.net/support/csc/swdist-domestic/ (customers in the United States and Canada)
   - https://www.juniper.net/support/csc/swdist-ww/ (all other customers)
2. Log in to the Juniper Networks Web site using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Using the J-Web interface or the CLI, select the appropriate JUNOS software with enhanced services image for your application. For information about JUNOS software with enhanced services packages, see "Upgrade and Downgrade Overview" on page 11.
4. Download JUNOS software with enhanced services to a local host or to an internal software distribution site.

Installing Software Upgrades with the J-Web Interface

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software upgrades from a remote server using FTP or HTTP, or by uploading the software image to the router. This section contains the following topics:

- Installing Software Upgrades from a Remote Server on page 13
- Installing Software Upgrades by Uploading Files on page 14

Installing Software Upgrades from a Remote Server

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software packages on the router that are retrieved with FTP or HTTP from the location specified. Installing software upgrades using this method copies the software image to the router.

NOTE: This procedure applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software Migration Guide*.

To install software upgrades from a remote server:

1. Download the software package as described in "Downloading Software Upgrades from Juniper Networks" on page 13.
2. In the J-Web interface, select **Manage > Software > Install Package**.

3. On the Install Package Quick Configuration page, enter information into the fields described in Table 3 on page 14.
4. Click **Fetch and Install Package**. The software is activated after the router reboots.

Table 3: Install Package Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name.	Type the full address of the software package location server—one of the following: ftp://*hostname/pathname/package-name* http://*hostname/pathname/package-name*
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	If this box is checked, the router is automatically rebooted when the upgrade is complete.	Check the box if you want the router to reboot automatically when the upgrade is complete.

Installing Software Upgrades by Uploading Files

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software packages uploaded from your computer to the router.

NOTE: This procedure applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software Migration Guide*.

To install software upgrades by uploading files:

1. Download the software package as described in "Downloading Software Upgrades from Juniper Networks" on page 13.
2. In the J-Web interface, select **Manage > Software > Upload Package**.
3. On the Upload Package page, enter information into the fields described in Table 4 on page 14.
4. Click **Upload Package**. The software is activated after the router has rebooted.

Table 4: Upload Package Summary

Field	Function	Your Action
File to Upload (required)	Specifies the location of the software package on the local system.	Type the location of the software package, or click **Browse** to navigate to the location.

Table 4: Upload Package Summary *(continued)*

Field	Function	Your Action
Reboot If Required	If this box is checked the router is automatically rebooted when the upgrade is complete.	Select the check box if you want the router to reboot automatically when the upgrade is complete.

Installing Software Upgrades with the CLI

This section contains the following topics:

- Installing Software Upgrades by Downloading Files on page 15
- Installing Software Upgrades from a Remote Server on page 16

Installing Software Upgrades by Downloading Files

To install software upgrades by downloading files to the router:

1. Download the JUNOS software with enhanced services package to the router using the following command:

   user@host> **file copy *source destination***

   Replace *source* with one of the following paths:

   - ftp://*hostname/pathname/package-name*

     or

   - http://*hostname/pathname/package-name*

   Replace *destination* with the path to the destination directory on the router. We recommend the /var/tmp directory.

2. Install the new package on the Services Router, entering the following command in operational mode in the CLI:

   user@host> **request system software add validate unlink no-copy *source***

   Replace *source* with */pathname/package-name* (for example, /var/tmp/junos-jsr-8.5R2.1.tar.gz).

   By default, the request system software add command uses the validate option to validate the software package against the current configuration as a prerequisite to adding the software package. This validation ensures that the router can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

   The unlink option removes the package at the earliest opportunity so that the router has enough room to complete the installation.

   (Optional) The no-copy option specifies that a software package is installed, but a copy of the package is not saved. Include this option if you do not have enough

space on the compact flash to perform an upgrade that keeps a copy of the package on the router.

3. After the software package is installed, reboot the router:

   user@host> **request system reboot**

   When the reboot is complete, the router displays the login prompt.

Installing Software Upgrades from a Remote Server

To install the software upgrades from a remote server:

1. Install the JUNOS software with enhanced services package on the Services Router, entering the following command in operational mode in the CLI:

   user@host> **request system software add validate unlink no-copy *source***

   Replace *source* with one of the following paths:

   - ftp://*hostname/pathname/package-name*

     or

   - http://*hostname/pathname/package-name*

   By default, the request system software add command uses the validate option to validate the software package against the current configuration as a prerequisite to adding the software package. This validation ensures that the router can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

   The unlink option removes the package at the earliest opportunity so that the router has enough room to complete the installation.

   (Optional) The no-copy option specifies that a software package is installed, but a copy of the package is not saved. Include this option if you do not have enough space on the compact flash to perform an upgrade that keeps a copy of the package on the router.

2. After the software package is installed, reboot the router:

   user@host> **request system reboot**

   When the reboot is complete, the router displays the login prompt.

Downgrade Instructions

This section contains the following topics:

- Downgrading the Software with the J-Web Interface on page 17
- Downgrading the Software with the CLI on page 17

NOTE: Juniper Networks supports direct software downgrades for a maximum of three releases.

Downgrading the Software with the J-Web Interface

You can downgrade the software from the J-Web interface. For the changes to take effect, you must reboot the router.

NOTE: This procedure applies only to downgrading one release of JUNOS software with enhanced services to another. To downgrade JUNOS software with enhanced services to the JUNOS software, see the *JUNOS Software Migration Guide*.

To downgrade software with the J-Web interface:

1. In the J-Web interface, select **Manage > Software > Downgrade**. The image of the previous software version (if any) is displayed on this page.

NOTE: After you perform this operation, you cannot undo it.

2. Select **Downgrade** to downgrade to the previous version of the software or **Cancel** to cancel the downgrade process.
3. When the downgrade process is complete, for the new software to take effect, click **Manage > Reboot** from the J-Web interface to reboot the router.

After you downgrade the software, the previous release is loaded, and you cannot reload the running version of software again. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image of JUNOS software with enhanced services labeled with the appropriate release.

Downgrading the Software with the CLI

You can revert to the previous version of software using the request system software rollback command in the CLI. For the changes to take effect, you must reboot the router. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image of JUNOS software with enhanced services labeled with the appropriate release.

NOTE: This procedure applies only to downgrading one release of JUNOS software with enhanced services to another. To downgrade JUNOS software with enhanced services to the JUNOS software, see the *JUNOS Software Migration Guide*.

To downgrade software with the CLI:

1. Enter the request system software rollback command to return to the previous JUNOS software version:

```
user@host> request system software rollback
```

The previous software version is now ready to become active when you next reboot the router.

2. Reboot the router:

```
user@host> request system reboot
```

The router is now running the previous version of the software. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image of JUNOS software with enhanced services labeled with the appropriate release.

List of Technical Publications

The following sections list hardware and software guides and release notes for J-series Services Routers running JUNOS software with enhanced services.

All documents are available at http://www.juniper.net/techpubs/.

Hardware Guides

- *J Series Services Routers Quick Start*—Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
- *J Series Services Routers Hardware Guide*—Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.

Software Guides

- *JUNOS Software Interfaces and Routing Configuration Guide*—Explains how to configure SRX-series and J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
- *JUNOS Software Security Configuration Guide*—Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP).
- *JUNOS Software Administration Guide*—Shows how to monitor SRX-series and J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
- *JUNOS Software CLI Reference*—Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices.
- *JUNOS Network Management Configuration Guide*—Describes enterprise-specific MIBs for JUNOS software. The information in this guide is applicable to M-series, T-series, EX-series, SRX-series, and J-series devices.

- *JUNOS System Log Messages Reference*—Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message. The information in this guide is applicable to M-series, T-series, EX-series, SRX-series, and J-series devices.
- *Network and Security Manager: Configuring J Series Services Routers and SRX Series Services Gateways Guide*—Explains how to configure, manage, and monitor J-series Services Routers and SRX-series services gateways through NSM.
- *JUNOS Software Design and Implementation Guide*—Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS software with enhanced services.
- *JUNOS Software Migration Guide*—Provides instructions for migrating an SSG device running ScreenOS software or a J-series Services Router running the JUNOS software to JUNOS software with enhanced services.
- *WXC Integrated Services Module Installation and Configuration Guide*—Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.

Release Notes

- *JUNOS Software Release Notes*—Summarize new features and known problems for a particular release of JUNOS software, including JUNOS software for J-series and SRX-series devices. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.

- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the gzip utility, rename the file to include your company name, and copy it to ftp.juniper.net:pub/incoming. Then send the filename, along with software version information (the output of the show version command) and the configuration, to support@juniper.net. For documentation issues, fill out the bug report form located at https://www.juniper.net/cgi-bin/docbugreport/.

Revision History

May 2009—Revision 4, Release 9.2R4 of JUNOS software with enhanced services.

January 2009—Revision 3, Release 9.2R3 of JUNOS software with enhanced services.

September 2008—Revision 2, Release 9.2R2 of JUNOS software with enhanced services.

August 2008—Revision 1, Release 9.2R1 of JUNOS software with enhanced services.

Copyright © 2009, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.